PERANCANGAN DAN IMPLEMENTASI SISTEM INFORMASI AKADEMIK BERBASIS *WEB* DI SMK 1 SATU MARET GARUT (BAGIAN KEAMANAN SISTEM TERBUKA)

DESIGN AND IMPLEMENTATION OF ACADEMIC INFORMATION SYSTEM BASED ON WEB IN SMK 1 SATU MARET GARUT (SECURITY OPEN SYSTEM PART)

Moch. Faisal Ikbal [1], Burhanuddin Dirgantara, Ir.MT [2], Fairuz Azmi,S.T.,M.T. [3]
[123] Prodi S1 Sistem Komputer, Universitas Telkom Bandung
[1]faisal.ikbal1993@gmail.com, [2]burhanuddin@telkomuniversity.ac.id , [3]worldliner@telkomuniversity.ac.id

Abstak

Penggunaan sistem informasi sangat dibutuhkan di zaman modern ini oleh institusi pendidikan, sistem informasi sangat membutuhkan sistem keamanan yang sanggup menjaga kerahasiaan data-data penting, begitu juga dengan Sistem Informasi untuk SMK 1 Satu Maret Garut yang juga memerlukan sistem keamanan. Segala bentuk penyalahgunaan *internet* karena adanya serangan dari *Hacker* membahayakan keamanan data-data yang bersifat sensitif , maka dari itu diperlukan sistem keamanan yang mampu mengetahui gangguan penyalahgunaan *internet. Intrusion Detection System* (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan). *Intrusion Prevention System* (IPS) merupakan kombinasi antara fasilitas *blocking capabilities* dari *firewall* dan kedalaman inspeksi paket data dari *Intrusion Detection System* (IDS). Dari kedua aplikasi tersebut diharapkan untuk bisa mencegah dan mengamankan data-data yang bersifat sensitif dari *hacker* yang mencoba masuk kedalam jaringan.

Kata kunci : Intrusion Detection System, Intrusion Prevention System (IPS) ,*Hacker, firewall , blocking capabilities* .

Abstract

The use of information systems is needed in modern times by educational institutions, information systems urgently need a security system capable of maintaining the confidentiality of sensitive data, as well as Information Systems for The SMK 1 Garut March that also requires security system. Any abuse of the internet for their attacks Hackers jeopardize the security of the data that is sensitive, it is necessary to know the security system that is capable of internet abuse disorders. Intrusion Detection System (IDS) is a software application or hardware device that can detect suspicious activity in a system or network. IDS can inspect inbound and outbound traffic in a system or network, perform analysis and search for evidence of attempted intrusion (intrusions). Intrusion Prevention System (IPS) is a combination between the amenities of a firewall blocking capabilities and depth of data packet inspection of Intrusion Detection System (IDS). Of both applications is expected to be able to prevent and secure the data-sensitive data from hackers trying to break into the network.

***keyword : Intrusion Detection System, Intrusion Prevention System (IPS) , Hacker, firewall, blocking capabilities* .**

1. Pendahuluan

Di zaman teknologi yang sedang berkembang ini Kehadiran Sistem Informasi sangat berguna untuk pengaksesan informasi dengan cepat,mudah,efisien dan akurat. Sistem Informasi adalah sebuah program/sistem yang mengatur data secara masal dengan menggunakan databases sebagai tempat penyimpanan data. Sistem Informasi sangat rentan terhadap serangan dari hacker, baik serangan melalui jaringan maupun serangan dari dalam . Pengertian Sistem Informasi Menurut Para Ahli - Secara umum Sistem informasi dapat didefinisikan sebagai suatu sistem di dalam suatu organisasi yang merupakan kombinasi dari orang-orang, fasilitas, teknologi, media prosedur-prosedur dan pengendalian yang ditujukan untuk mendapatkan jalur komunikasi penting, memproses tipe transaksi rutin tertentu, memberi sinyal kepada manajemen dan yang lainnya terhadap kejadian-kejadian internal dan eksternal yang penting dan menyediakan suatu dasar informasi untuk pengambilan keputusan.[2]

Berdasarkan Latar belakang diatas maka dianggap perlu sebuat sistem keamanan sistem terbuka yang berguna untuk mengamankan data-data dalam sebuah server melalui control

jaringan. Dari masalah tersebut maka Penulis berniat membuat "Perancangan dan Implementasi Sistem Informasi Akademis Berbasis Web di SMK 1 Satu Maret Garut Bagian Keamanan Sistem Terbuka ". Diharapkan Sistem keamanan ini dapat melindungi data-data dari sistem informasi melalui jaringan SMK 1 Maret Garut.

2. Material dan Metodologi

2.1 IDS (Intrusion Detection System)

Intrusion Detection System adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan

intrusi (penyusupan).

IDS *Intrusion Detection System* adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap *traffic* yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP (*Internet Protocol*).

2.2 IPS *(Intrusion Prevention System)*

Intrusion Prevention System merupakan kombinasi antara fasilitas blocking capabilities dari Firewall dan kedalaman inspeksi paket data dari Intrusion Detection System (IDS). IPS diciptakan pada awal tahun 1990-an untuk memecahkan masalah serangan yang selalu melanda jaringan komputer. IPS membuat akses kontrol dengan cara melihat konten aplikasi, dari pada melihat IP address atau ports, yang biasanya dilakukan oleh firewall. IPS komersil pertama dinamakan BlackIce diproduksi oleh perusahaan NetworkIce, hingga kemudian berubah namanya menjadi ISS(Internet Security System). Sistem setup IPS sama dengan sistem setup IDS. IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Secara logic IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi sistem call.[3]

2.3 Snort

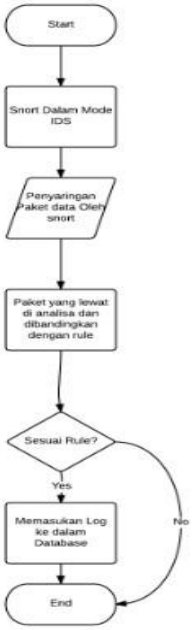
Snort adalah sebuah software ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu Network IntrusionDetection System (NIDS) yang berskala ringan (lightweight), dan software inimenggunakan sistem peraturan-peraturan (rules system) yang relatif mudah dipelajariuntuk melakukan deteksi dan pencatatan (logging) terhadap berbagai macam seranganterhadap jaringan komputer.

Dengan membuat berbagai rules untuk mendeteksi ciri-cirikhas (signature) dari berbagai macam serangan, maka Snort dapat mendeteksi danmelakukan logging terhadap serangan-serangan tersebut. Software ini bersifat opensource berdasarkan GNU General Public License [GNU89], sehingga boleh digunakan dengan bebas secara gratis, dan kode sumber (source code) untuk Snort jugabisa didapatkan dan dimodifikasi sendiri bila perlu. Snort pada awalnya dibuat untuk sistem operasi (operating system) berdasarkan Unix, tetapi versi Windows juga sudahdibuat sehingga sekarang ini Snort bersifat cross-platform.Snort sendiri merupakan software yang masih berbasis command-line, sehingga cukupmerepotkan bagi pengguna yang sudah terbiasa dalam lingkungan Graphical UserInterface (GUI).

Oleh karena itu, ada beberapa software pihak ketiga yang memberikanGUI untuk Snort, misalnya IDScenter untuk Microsoft Windows, dan Acid yangberbasis PHP sehingga bisa diakses melalui web browser.[2]

3. Pembahasan

3.1 Gambaran Umum Sistem



Gambar 3.1 Flowchart Desain Utama

Sistem yang dibangun adalah Intrusion Prevention System Berbasis sebuat system yang menggunakan software open source yaitu Snort. Semua paket-paket yang melewati jaringan akan disaring dengan rule-rule yang ada pada Snort sehingga ketika sebuah penyerangan terjadi dan tersaring oleh rule, paket tersebut akan di drop menggunakan firewall dan rule tersebut tersimpan didalam log database.

3.2 Perangkat Keras

Dalam membangun sistem keamanan ini digunakan perangkat keras dengan spesifikasi sebagai berikut:

a. Server
- CPU : Pentium 4(1GHz)
- RAM: 512MB
- Hardisk: 128GB

b. Penyerang /Attacker
- Sebuah Notebook yang mempunyai Network Interface Card

c. Perangkat lainnya
- Switch TPLink 8 port
- Kabel utp cat 11 buah

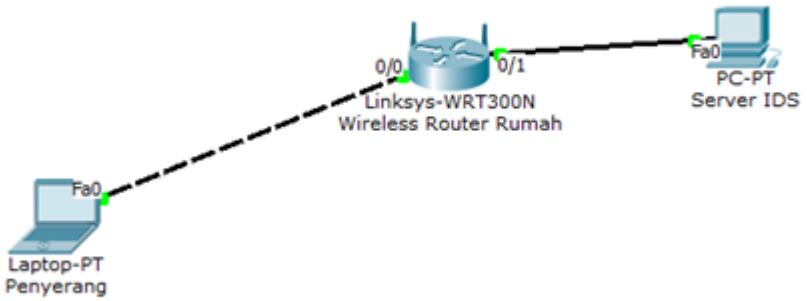
3.3 Perangkat Lunak

Adapun perangkat lunak yang digunakan dalam pembuatan penelitian Tugas Akhir ini adalah sebagai berikut:

- Linux Debian Ubuntu 14.04 LTS sebagai server.
- Snort sebagai analisa protokol ,penyaringan paket, pembanding dengan rule yang ada.
- MySQL sebagai tempat hasil penyaringan data oleh Snort.

3.4 Topologi Jaringan

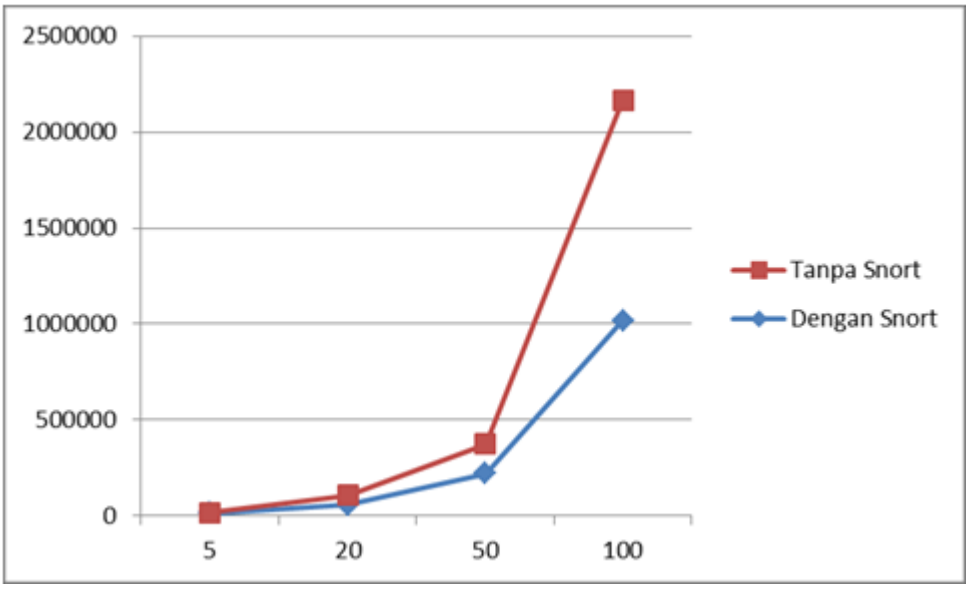
Pemodelan Topologi yang merupakan perancangan dalam pengujian .



Gambar 3.4 Topologi Jaringan

3.5 Time Spent Perbandingan Dengan dan Tanpa Snort

Berdasarkan Gambar 3.5 telihat jika aplikasi tanpa menggunakan snort lebih bagus performansinya dibandingkan menggunakan snort, tetapi saat menggunakan snort perbandingannya tidak terlalu jauh dibanding tidak menggunakan snort.



Gambar 3.5 Time Spent

3.6 Pengujian Scanner Attack

Scanner merupakan kegiatan menyelidiki dengan menggunakan tools secara otomatis. Scanner bertujuan untuk mendapatkan informasi port yang terbuka pada sebuah server guna untuk bahan penyerangan berikutnya.

Tools yang digunakan disini adalah Nmap-Zenmap yang berada pada penyerang, untuk menggunakan tools tersebut penyerang harus lah mengetahui IP server yang telah ditargetkan terlebih dahulu sebelum menyerang , disini server menggunakan IP 192.168.1.12 , pada Nmap-

Zenmap masukan IP tersebut pada kolom target, kemudian pada profile pilih mode Intense Scan lalu click tombol scan untuk memulai scanning dan mendapat port-port yang terbuka.

Tabel 4. 1 Pengujian Nmap-Zenmap

Port	Protocol	IP Address	Status
443	**TCP**	**192.168.1.12**	**Open**
22	**TCP**	**192.168.1.12**	**Open**
111	**TCP**	**192.168.1.12**	**Open**
80	**TCP**	**192.168.1.12**	**Open**
5000	**TCP**	**192.168.1.12**	**Open**
8000	**TCP**	**192.168.1.12**	**Open**

Penyerang mendapatkan informasi mengenai *port* yamg terbuka antara lain *port* 22, 25, 80, 111, 443, 5000 dan 8000. Dengan informasi tersebut penyerang dapat melancarkan serangan.

Dengan Snort yang berjalan sebagai IDS , penyerangan tersebut dapat diketahui , penyerang ber IP 192.168.1.9 yang terlihat pada tabel.

Tabel 4. 2 Alert Snort Scan Attack

waktu	IP Source	IP Destination	Port	Message Alert
29/4 – 09:51:07	**192.168.1.9**	**192.168.1.12**	**80**	**Consecutive TCP small Segments exceeding**
29/4 – 09:51:09	**192.168.1.9**	**192.168.1.12**	**80**	

3.7 Pengujian Ping Attack

Ping attack merupakan salah satu serangan DoS attack yang paling terkenal karena mudah dilakukan. Hanya menggunakan utility ping, DoS dapat dilakukan.
Kinerja Ping Attack dengan mengirimkan paket 65.536 byte ping merupakan sesuatu yang ilegal dalam protokol jaringan, tetapi paket ini dapat dikirim secara terpecah-belah. Ping attack ini bertujuan membuat server menjadi berat dan crash.

Penyerang menggunakan command promp , lalu memasukan command dengan mengirimkan paket yang besar dengan alamat IP server yaitu :
Ping 192.168.1.12 –I 500 –t

Tabel 4. 3 Penyerangan IP

IP Source	IP Destination	Time	Bytes	TTL
192.168.1.9	**192.168.1.12**	**<1ms**	**500**	**64**

Tabel 4. 4 Snort Detected IP Attack

waktu	IP Source	IP Destination	Port	Protocol	Priority	Message
29/4 – 06:02:015	**192.168.1.9**	**192.168.1.12**	**80**	**ICMP**	**3**	**ICMP Test Detected**
29/4 – 06:02:018	**192.168.1.9**	**192.168.1.12**	**80**	**ICMP**	**3**	**ICMP Test Detected**

Tabel diatas menunjukkan terjadinya serangan Ping attack yang tertangkap pada Snort IDS mode , ping attack termasuk penyerangan kelas berat yang dapat menyebabkan terjadinya server down , terlihat pada gambar menunjukan *priority* :3.

3.8 Pengujian TCP Attack

Penyerang menggunakan Tools yang bernama LOIC (*Low Orbital Ion Cannon)* yang berfungsi sebagai permintaan pengiriman paket secara berlebihan yang membanjiri server pada saat server beraktifitas . Tujuan TCP Attack ini membuat server menjadi berat dan hang saat beroperasi.
Cara menggunakan LOIC adalah dengan memasukan IP pada kolom IP lalu klik tombol lock on untuk mengunci IP target , setelah IP yang akan diserang muncul di aplikasi, maka kita setting Method TCP yang akan digunakan, lalu klik ready untuk memulai DoS menggunakan Protokol TCP.
Penyerangan tersebut dideteksi dengan Snort IPS mode (inline) dengan gambar dibawah ini, gambar tersebut medapati adanya anomali-anomali yang terjadi pada jaringan jangkauan perlindungan snort, Paket yang didapati sebagai serangan tersebut langsung di drop.

Tabel 4. 5 Snort IPS Mode Dropped Packet

IP Source	IP Destination	Protocol	Port	Message	Received Packet	Analyed Packet	Dropped Packet
192.168.1.9	**192.168.1.12**	**TCP**	**35352**	**Consecutive TPC small Segment Excending**	**171037**	**766 (0,448%)**	**19823727 (99,552%)**

Paket yang dinyatakan sebagai serangan oleh Snort akan di drop , sehingga server tidak merasa terbanjiri dengan permintaan pengiriman data yang berlebihan, paket di drop terlihat pada gambar dibawah ini
Pada gambar diatas pada bagian Packet I/O Totals: telihat bahwa data
Received : 171037
Analyzed : 766 (0,448%)
Dropped : 19823727 *(99,552%)* = 19823727 *x 1000bytes = 19,8 GB*
Dari data tersebut maka disimpulkan bahwa paket yang berupa serangan DoS di Drop *(99,552%)* dari paket yang masuk pada sistem I/O .

3.9 Pengujian UDP Attack

Penyerang menggunakan Tools yang sama dengan saat menyerang server menggunakan TCP Attack, tugas utama UDP Attack adalah membuat server merasa berat karena kehabisan sumber daya dikarenakkan permintaan paket UDP yang banyak dalam satu waktu, cara yang digunakan penyerang hanya mengganti mode TCP menjadi UDP pada tools LOIC.

Tabel 4. 6 Pengujian UDP

IP Source	IP Destination	Protocol	Port	Attack Type	Time	Packet Requested
192.168.1.9	**192.168.1.12**	**UDP**	**80**	**DoS**	**2 minute 50 seconds**	**13094305**

Dengan menggunakan Snort IPS, penyerangan tersebut langsung ditanggapi dan didrop setiap paket yang dianggap menyerang server, gambar dibawah ini menunjukan terjadinya serangan ke server.
Snort IPS mode menangkap adanya serangan yang terjadi pada server, selanjutnya snort menindaklanjuti serangan tersebut dengan mendrop semua paket yang dianggap ancaman.

Tabel 4. 7 Snort Drop UDP Attack

IP Source	IP Destination	Protocol	Port	Message	Received Packet	Analyed Packet	Dropped Packet
192.168.1.9	**192.168.1.12**	**UDP**	**35352**	**Consecutive TPC small Segment Excending**	**169669**	**129 (0,076%)**	**14961743 (98,879%)**

Dari gambar tersebut telihat jumlah paket yang di drop oleh Snort IPS mode sekitar 98% dari paket yang masuk kedalam jaringan Snort.

3.10 Pengujian HTTP Attack

HTTP Attack merupakan serangan DoS yang Umum dan mudah dilakukan , HTTP Attack menggunakan teknik download data yang berada di server secara berlebihan sehingga server menjadi down.

Tabel 4. 8 HTTP Attack

IP Source	IP Destination	Protocol	Port	Attack Type	Time	Packet Downloaded
192.168.1.9	**192.168.1.12**	**HTTP**	**80**	**DoS**	**1 minute 05 seconds**	**5757**

Gambar diatas adalah penyerang menggunakan applikasi loic untuk menyerang server , terlihat applikasi mendownload 5757 data dalam waktu beberapa detik .

Tabel 4. 9 Snort Drop HTTP Attack

IP Source	IP Destination	Protocol	Port	Message	Received Packet	Analyed Packet	Dropped Packet
192.168.1.9	**192.168.1.12**	**HTTP**	**1900**	**Consecutive TPC small Segment Excending**	**669**	**59 (0,046%)**	**61743 (93,709%)**

Tabel diatas menyatakan bahwa snort menyadari adanya serangan yang terjadi pada server. Paket-paket yang melebihi batas wajar telah di drop oleh snort IPS mode .

3.11 SynFIN Attack

Serangan SynFIN dengan cara mengirim kan Flag FIN sebagai sekumpulan byte dari data. Penyerang menggunakan tools Nmap-Zenmap , kemudian memasukkan IP target pada command tuliskan perintah

Nmap –sF –T4 –O –PS 192.168.1.12

Tabel 4. 10 SynFIN Attack

Port	Protocol	IP Address	Service
443	**TCP**	**192.168.1.12**	**https**
22	**TCP**	**192.168.1.12**	**ssh**
111	**TCP**	**192.168.1.12**	**rpcbind**
80	**TCP**	**192.168.1.12**	**http**
5000	**TCP**	**192.168.1.12**	**upnp**
8000	**TCP**	**192.168.1.12**	**http-alt**

Dari penyerangan tersebut tools mengirimkan bit TCP FIN (-sF) , Aggressive (- T4) , Operating system detection (-O), Syn Ping (-PS).

Tabel 4. 11 Snort Detect SynFIN

IP Source	IP Destination	Protocol	Port	Header
192.168.1.9	**192.168.1.12**	**TCP**	**1900**	**.../.....rd..... .....Perspectivy-PC.....7...MSFT 5.0.....**

Serangan SynFIN dapat dideteksi oleh snort IPS mode, terlihat pada gambar diatas yang menunjukkan isi dari header paket yang menunjukkan nama PC penyerang.

4. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan beberapa poin sebagai berikut:

1. Implementasi sistem keamanan pada Sistem Informasi di SMK 1 Satu maret garut belum terlaksana dikarenakan belum adanya jaringan internet yang terpasang, tetapi sudah terancang dan sudah diuji berupa *prototype* .
2. Dilakukan pengujian terhadap snort sebanyak 6 kali :
    a) Pengujian Ping Attack dengan hasil ICMP Test Detected pada port 80 .
    b) Pengujian TCP Attack dengan hasil 171037 received packet, 766 (0,448%) analyed packet, 19823727 (99,552%) dropped packet.
    c) Pengujian UDP Attack dengan hasil 169669 received packet 129 (0.076%) analyed packet, 14961743 (98,879%) dropped packet.
    d) Pengujian HTTP Attack dengan hasil 669 received packet 59 (0.046%) analyed packet, 61743 (93,709%) dropped packet.
    e) Pengujian Scanner Attack dengan hasil Message Alert Consecutive TCP small Segments exceeding pada port 80.
    f) Pengujian SynFIN Attack dengan hasil header packet .../.....rd.....
.....Perspectivy-PC.....7...MSFT 5.0.....

Snort mendeteksi serangan yang diluncurkan oleh komputer penyerang yaitu Perspectivy-PC.
Penyerangan yang paling berpengaruh terhadap Snort adalah Penyerangan UDP Attack dikarenakan serangan tersebut mengirimkan lebih dari 15juta paket dalam 2 menit 50 detik.
Penyerangan yang paling lemah terhadap Snort adalah Scanner Attack karena penyerangan tersebut hanya sebatas melihat port yang terbuka dan tidak akan menyebabkan pengaruh yang besar terhadap server.

3. Snort berpengaruh terhadap performansi terbukti dengan menggunakan snort 5 user Time Spent 14.803ms, 20 user Time Spent 55.885ms , 50 user Time Spent 219.346ms , 100 user Time Spent 1.018.047ms sedangkan tidak menggunakan snort 5 user Time Spent 12.260ms, 20 user Time Spent 51.919ms , 50 user Time Spent 156.306ms , 100 user Time Spent 1.145.990ms artinya

DAFTAR PUSTAKA

[1] Miftahul, Jannah. 2012. ***Implementasi IDS SNORT pada laboratorium Jaringan Kompiuter.***.

[2] Jane P. Laudon, Kenneth C. Laudon 2015 ***Management Information System (Managing Digital Firm), 12th*** . Prentice-Hall Inc.

[3] Noah Diestrich. 2015 ***Snort 2.9.8.x on Ubuntu 12, 14, 15,*** diakses pada 17-09-2015, pada pukul 04.39 WIB.

[4] Rehman, . 2003. ***Intrusion Detection withSNORT: Advanced IDS TechniquesUsing SNORT, Apache, MySQL, PHP,and ACID.*** Prentice Hall of New Jersey.

[5] Tanenbaum ,Andrew S. 2006. ***Computer Networks. 2nd Edition***. Prentice Hall

[6] *Jin Yu, Eun. 2009.* ***Network Intrusion Detection Systems for High Security Networkings. IJCSNS International Journal of Computer Science and Network Security****, VOL.9 No.10,*

[7] *J.Postel, .Wilson Bolevard 1981.* ***Defense Advanced Research Projects Agency Information Processing Techniques Office****, Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey,California.*